D-MATH Algebra I HS20
Prof. Manfred Einsiedler

Lösung 4

Quotientenkörper, Polynomringe, Ideale

1. Sei R ein Integritätsbereich und $f, g \in R \smallsetminus \{0\}$. Seien d, d' zwei grösste gemeinsame Teiler von f und g. Zeigen Sie, dass es eine Einheit $c \in R^\times$ gibt, so dass $d = cd'$. In anderen Worten, ein grösster gemeinsamer Teiler ist bis auf Multiplikation mit einer Einheit eindeutig.

2. Sei n eine positive natürliche Zahl. Bestimmen Sie alle invertierbaren Elemente im Ring $\mathbb{Z}[\sqrt{-n}] = \mathbb{Z} + \sqrt{-n}\mathbb{Z} \subseteq \mathbb{C}$.

   Hinweis: Benutzen Sie eine Normfunktion.

3. Sei R ein kommutativer Ring und sei $\mathrm{Mat}_{nn}(R)$ der Ring der $n \times n$-Matrizen mit Koeffizienten in R mit der üblichen Addition und Multiplikation.

   Definition: Sei S ein nichtkommutativer Ring. Ein *zweiseitiges Ideal in S* ist eine Teilmenge $J \subseteq S$ so dass $0 \in J$ und $j, j' \in J \implies j + j' \in J$ und $j \in J$, $s \in S \implies js, sj \in J$.

   (a) Zeigen Sie: Ist $I \subseteq R$ ein Ideal, so ist

   $$\mathrm{Mat}_{nn}(I) := \{M = (m_{ij})_{1 \leqslant i,j \leqslant n} \in \mathrm{Mat}_{nn}(R) | m_{ij} \in I \text{ für alle } 1 \leqslant i, j \leqslant n\}$$

   ein zweiseitiges Ideal in $\mathrm{Mat}_{nn}(R)$.

   (b) Zeigen Sie: Jedes zweiseitige Ideal in $\mathrm{Mat}_{nn}(R)$ ist von der Form $\mathrm{Mat}_{nn}(I)$ für ein geeignetes Ideal $I \subseteq R$.

   Bemerkung: Ist J ein zweiseitiges Ideal in einem nicht-kommutativen Ring S, dann hat S/J wieder eine Ringstruktur. In unserem Beispiel kann man sogar zeigen, dass $\mathrm{Mat}_{nn}(R/I) \cong \mathrm{Mat}_{nn}(R)/\mathrm{Mat}_{nn}(I)$, also, dass der Faktorring wieder ein Matrixring über einem kommutativen Ring ist.

4. (a) (**SAGE**) Schreiben Sie eine Method in SAGE, die den euklidischen Algorithmus implementiert und daher den grössten gemeinsamen Teiler von zwei Elementen berechnet.

   Hinweis: Verwenden Sie hierzu %, um den Rest der Division zu bestimmen. Überspringen Sie Schritt 0 in der Definition des euklidischen Algorithmus, da es keine Rolle spielt und dies die Implementierung einer Normfunktion verhindert. (Frage: Warum?)

(b) Verifizieren Sie mit der obigen Methode Ihre Rechnungen in der Aufgabe 5 (a)-(d).

Hinweis: Hilfreiche Stichwörter, nach denen Sie im Sage Handbuch suchen können: PolynomialRing, FractionField, GF (steht für Galois field). Bei der Verifikation von Aufgabe 5 (d) gibt es Probleme bei der Benutzung von %, falls eines der Argumente des euklidischen Algorithmus' die Variable T ist (dies gibt einen Fehler obwohl T eine Einheit in $K[X]$ ist, % sollte also 0 ausgeben). Sie können diesen Fehler vermeinden, indem Sie vor Anwendung von % überprüfen, ob die Argumente Einheiten sind, und in diesem Fall das richtige Ergebnis direkt ausgeben lassen. Wichtig ist hierbei zu beachten, dass T als Element verschiedener Ringe aufgefasst werden kann und nicht in allen eine Einheit ist.

5. (a) Betrachten Sie die Polynome $p, q \in \mathbb{Q}[X]$ definiert durch

$$p := X^3 - \frac{5}{2}X^2 + \frac{3}{2}X \text{ und } q := 2X^2 - X - 3.$$

Berechnen Sie die Division mit Rest von p durch q.

(b) Finden Sie einen Erzeuger des Hauptideals $(p, q) \subseteq \mathbb{Q}[X]$.

(c) Benutzen Sie Division mit Rest in $\mathbb{F}_3[X]$, wobei $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ der Körper mit drei Elementen ist, um zu zeigen, dass die Ideale $(X^4 + 2X + 1)$ und $(X^2 + X - 1)$ in $\mathbb{F}_3[X]$ koprim sind.

Erinnerung: Zwei Ideale $I, J \subseteq R$ in einem Ring R heissen koprim, falls $I + J = R$.

(d) Sei $K = \mathbb{Q}(T)$. Berechnen Sie die Division mit Rest in $K[X]$ von

$$f := X^3 + TX^2 - 1 \text{ durch } g := (1 + T)X^2 - 1.$$

Lösung:

(a) Wir berechnen die Division mit Rest von p durch q.

$$\begin{aligned} X^3 - \frac{5}{2}X^2 + \frac{3}{2}X &= \frac{1}{2}X(2X^2 - X - 3) + \frac{1}{2}X^2 + \frac{3}{2}X - \frac{5}{2}X^2 + \frac{3}{2}X \\ &= \frac{1}{2}X(2X^2 - X - 3) - 2X^2 + 3X \\ &= \left(\frac{1}{2}X - 1\right)(2X^2 - X - 3) - X - 3 + 3X \\ &= \left(\frac{1}{2}X - 1\right)(2X^2 - X - 3) + 2X - 3 \end{aligned}$$

und wir erhalten den Nenner $\frac{1}{2}X - 1$ und den Rest $2X - 3$.

(b) Aus (a) wissen wir, dass

$$\left(X^3 - \frac{5}{2}X^2 + \frac{3}{2}X, 2X^2 - X - 3\right) = (2X^2 - X - 3, 2X - 3) \subset \mathbb{Q}[X].$$

Wir führen eine weitere Division mit Rest durch:

$$2X^2 - X - 3 = X(2X - 3) + 3X - X - 3 = (X + 1)(2X - 3),$$

und daraus folgt, dass $\left(X^3 - \frac{5}{2}X^2 + \frac{3}{2}X, 2X^2 - X - 3\right) = (2X - 3) \subset \mathbb{Q}[X]$.

(c) Wir berechnen die Division mit Rest von $X^4 + 2X + 1$ durch $X^2 + X - 1$ in $\mathbb{F}_3[X]$:

$$\begin{aligned} X^4 + 2X + 1 &= X^2(X^2 + X - 1) - X^3 + X^2 + 2X + 1 \\ &= (X^2 - X)(X^2 + X - 1) + X^2 - X + X^2 + 2X + 1 \\ &= (X^2 - X + 2)(X^2 + X - 1) - 2X + 2 + X + 1 \\ &= (X^2 - X + 2)(X^2 + X - 1) + 2X. \end{aligned}$$

Daraus folgt, dass $(X^4 + 2X + 1, X^2 + X - 1) = (X^2 + X - 1, -X) = (X^2 + X - 1, X) = (-1, X) = (-1) = \mathbb{F}_3[X]$, und damit auch, dass die zwei Ideale koprim sind.

(d) Wir benutzen den euklidischen Algorithmus über dem Körper der rationalen Funktion $\mathbb{Q}(T)$.

$$\begin{aligned} f = X^3 + TX^2 - 1 &= \frac{1}{1+T}X((1+T)X^2 - 1) + \frac{1}{1+T}X + TX^2 - 1 \\ &= \left(\frac{1}{1+T}X + \frac{T}{1+T}\right)((1+T)X^2 - 1) + \frac{1}{1+T}X - 1 + \frac{T}{1+T} \\ &= \left(\frac{1}{1+T}X + \frac{T}{1+T}\right)g + \frac{1}{1+T}X - \frac{1}{1+T}. \end{aligned}$$

6. Sei K ein unendlicher Körper.

(a) Angenommen $P \in K[X]$ ist ein Polynom, so dass $P(\alpha) = 0$ für alle $\alpha \in K$ gilt. Zeigen Sie, dass $P = 0$ in $K[X]$.

(b) Angenommen $P \in K[X_1, \ldots, X_n]$ ist ein Polynom, so dass $P(\alpha) = 0$ für alle $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$ gilt. Zeigen Sie, dass $P = 0$ in $K[X_1, \ldots, X_n]$.
Hinweis: Machen Sie eine Induktion über n und benutzen Sie Aufgabenteil (a).

Lösung:

(a) Wir zeigen zuerst, dass die Anzahl von Nullstellen von P kleiner gleich der Grad von P ist durch Induktion über den Grad. Dies ist wahr für Polynome vom Grad 0 und 1. Wir nehmen an, die Aussage ist wahr für Polynome vom Grad $n-1$. Hat P keine Nullstelle in K ist die Aussage wahr. Ist $\alpha \in K$ eine Nullstelle von P, dann gilt nach Division mit Rest, dass $P(X) = (X-\alpha)Q(X)$ für ein Polynom Q vom Grad $n-1$. Da $P(\beta) = 0$ genau dann, wenn $\alpha = \beta$ oder $Q(\beta) = 0$, folgt nach Induktionsannahme, dass P höchstens n Nullstellen hat.

Angenommen $P \neq 0$. Nach der obigen Überlegung folgt, dass P weniger als $\deg(P)$ Nullstellen hat. Da jedes Element $\alpha \in K$ eine Nullstelle ist und K unendlich, folgt, dass $\infty = |K| \leqslant \deg(P) < \infty$, was ein Widerspruch ist.

(b) Wir beweisen dies durch Induktion über n, wobei $n = 1$ aus (a) folgt. Angenommen die Aussage gilt für $n-1$. Sei $d = \deg_{X_n}(P)$ und $a_i \in K[X_1, \ldots, X_{n-1}]$, so dass

$$P(X_1, \ldots, X_n) = \sum_{i=0}^{d} a_i(X_1, \ldots, X_{n-1}) X_n^i.$$

Für jedes $(\alpha_1, \ldots, \alpha_{n-1}) \in K^{n-1}$ definieren wir

$$q_{\alpha_1,\ldots,\alpha_{n-1}}(Y) = P(\alpha_1, \ldots, \alpha_{n-1}, Y) = \sum_{i=0}^{d} a_i(\alpha_1, \ldots, \alpha_{n-1}) Y^i \in K[Y].$$

Nach Konstruktion gilt $q_{\alpha_1,\ldots,\alpha_{n-1}} \in K[Y]$ verschwindet auf allen Elementen in K. Aus (a) folgt, dass $q_{\alpha_1,\ldots,\alpha_{n-1}}(Y) = 0$, was nichts anderes bedeutet als dass für alle $i = 0, \ldots, d$ und $(\alpha_1, \ldots, \alpha_{n-1}) \in K^{n-1}$ $a_i(\alpha_1, \ldots, \alpha_{n-1}) = 0$. Nach Induktionsannahme (angewandt auf alle a_is) folgt $a_i = 0$, was impliziert, dass $P = 0$.